

REMARKS

In the Office Action, the Examiner indicated that claims 1 through 24 are pending in the application and the Examiner rejected all claims.

By this amendment, claims 1, 6, 9, 14, 17, and 22 have been amended to specifically recite the use of write-only storage, and claims 7, 15, and 23 have been canceled.

Claim Rejections, 35 U.S.C. §103

In item 2 on page 2 of the Office Action, the Examiner rejected claims 1-24 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 5,949,877 to Traw et al. ("Traw '877") in view of U.S. Patent No. 6,542,610 to Traw et al. ("Traw '610").

The Present Invention

The present invention allows the use of wireless devices containing a radio module to connect in a secure manner using digital certificates. The present invention does not require manual entry of user identifiers, passwords, or cryptographic keys. A private key is generated within the wireless device, and is immediately placed in *write-only storage* within the device, and cannot thereafter leave the write-only storage.

The term "write-only storage" is clearly defined in the specification, e.g., beginning on page 16, line 3. More specifically, the wireless device's private key is stored in that device using a write-only storage means, such that there is no way for software residing in the device to read the key but the device can execute operations against the information.

Using the “write-only storage” as defined in the specification, it is physically impossible for its contents to be read, ever. The protected storage, being a write-only memory, is not capable of emitting the private key value.

U.S. Patent No. 5,949,877 to Traw et al.

U.S. Patent No. 5,949,877 to Traw et al. teaches a method for protecting digital content from copying and/or other misuse as it is transferred between devices over insecure links. The storage of the key and the key exchange of Traw ‘877 is implemented in software (e.g., see Col. 3, lines 52-55; Col 4., lines 17-20). There is no teaching or suggestion of anything other than a standard, prior art system in which the private key is in a read/write memory accessible by software (i.e., read by the software to provide the security function of the private key).

U.S. Patent No. 6,542,610 to Traw et al.

U.S. Patent No. 6,542,610 to Traw et al. is a continuation-in-part of Traw ‘877 and contains essentially the same teachings as Traw ‘877 with respect to storage of and access to the private key. The Examiner appears to rely on Traw ‘610 for an alleged teaching of establishing an initial session between first and second devices and negotiating a two-way session encryption and mutual authentication requirements between the two devices.¹

¹ The Examiner again fails to identify which “Traw” reference is being referred to; Applicant cannot be sure that it has properly figured out which Traw reference is being referred to at any given point in the Office Action but has made a good-faith attempt to do so.

The Examiner has not Established a *prima facie* Case of Obviousness

As set forth in the MPEP:

To establish a *prima facie* case of obviousness, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skilled in the art, to modify the reference or to combine reference teachings.

MPEP 2143

As noted above, neither of the Traw patents (Traw '877 or Traw '610) teach or suggest the use of write-only storage as defined in the present invention. They simply teach traditional read/write memory used to store and access the private key. A traditional read-write storage *could* be designated for use in write operations only -- so long as one trusts that the software (or an unscrupulous user of the software) will never attempt to perform a read operation on the storage, and trusts that the system within which the storage resides will provide some tamper resistance. However, there is no suggestion or teaching of forever excluding the ability to read from the memory of Traw, and in fact, it can be read.

By contrast, the write-only storage of the present invention can NEVER be read; it is impossible. This write-only storage is specifically claimed in each independent claim. The write-only storage as claimed in the present invention is patentably distinct from the disclosures of either Traw patent, alone or in combination. Nothing in either Traw patent teaches or suggests the claimed invention.

The Examiner's conclusory assertion that the use of write-only storage is well known in the art and would render obvious the claimed inventions are incorrect and are improper under the law. Applicant refers the Examiner to *In re Sang-su Lee* (277 F.3d, 1338 Fed. Cir. 2002; 61 U.S.P.Q. 2d, 1430). "The Examiner's conclusory statements ... do not adequately

address the issue of motivation to combine. This factual question of motivation is material to patentability, and could not be resolved on subjective belief and unknown authority."

Both EEPROMs and DRAMs by definition will return a value that was written into them, and if that value is encrypted by a key, then one in possession of the key could recover the value. Like the prior art described in the present specification, using an EEPROM or DRAM for the storage function claimed does not solve the problem of how to protect the key ring from an attacker without also relying on a person supplying a secret to unlock the ring, and how to protect the user's secret while this process takes place.

As stated above and in the previous Response, it is well known that a traditional read-write storage *could* be designated for use in write operations only, but only as long as one trusts that the software (or an unscrupulous user of the software) will never attempt to perform a read operation on the storage, and trusts that the system within which the storage resides will provide some tamper resistance. Thus, the storage of the Traw patents is faulty in that it can be read.

By contrast, the protected storage of the present invention can NEVER be read; it is impossible.

Each of the independent claims of the present invention, as amended, specifically recites the write-only storage as defined in the specification of the present invention. Accordingly, all claims patentably define over the Traw patents. The Examiner is respectfully requested to reconsider and withdraw the rejection of claim 1-24 under 35 U.S.C. §103.

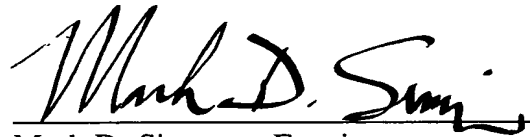
Conclusion

The present invention is not taught or suggested by the prior art. Accordingly, the Examiner is respectfully requested to reconsider and withdraw the rejection of the claims. An early Notice of Allowance is earnestly solicited.

The Commissioner is hereby authorized to charge any fees or credit any overpayment associated with this communication to Deposit Account No. 19-5425.

Respectfully submitted

1/29/04
Date


Mark D. Simpson, Esquire
Registration No. 32,942

SYNNESTVEDT & LECHNER LLP
2600 ARAMARK Tower
1101 Market Street
Philadelphia, PA 19107

Telephone: (215) 923-4466
Facsimile: (215) 923-2189